VZCZCXRO7773
PP RUEHAST RUEHBW RUEHFL RUEHLA RUEHMRE RUEHPOD RUEHROV RUEHSR
DE RUEHC #8469 1281850
ZNR UUUUU ZZH
P R 071844Z MAY 08
FM SECSTATE WASHDC
TO RUEHVEN/USMISSION USOSCE PRIORITY 0350
INFO ORG FOR SECURITY CO OP IN EUR COLLECTIVE

UNCLAS STATE 048469

SIPDIS

E.O. 12958: N/A
TAGS: OSCE PTER PREL
SUBJECT: OSCE PERMANENT COUNCIL: STATEMENT ON RECENT CYBER ATTACKS IN THE OSCE REGION

¶1. Post is authorized to present the following statement at the May 8 Permanent Council meeting in Vienna.

Begin text:

Mr. Chairman,

On April 26 the website of the Belarus Service of Radio Free Europe/Radio Liberty was the subject of a cyber attack. RFE/RL, which is an independent, international news and broadcast organization, is one of the few sources of outside information about developments in Belarus. Funded by the United States Congress through the Broadcasting Board of Governors, RFE/RL broadcasts enjoy broad listenership in Belarus and throughout the OSCE region. Many more people, however, rely on RFE/RL websites for the latest news and information about what is occurring inside their countries. When the two-day denial of service attack occurred, RFE,s Belarus Service was preparing special coverage of protests in Minsk on the anniversary of the 1986 Chernobyl disaster. The cyber attack was apparently intended to make the targeted website unavailable to its users; it quickly spread to several other RFE/RL websites.

According to RFE/RL, it has been hit before by denial-of-service attacks, which seek to flood a web-site with fake attempts to gain access in a deliberate effort to overwhelm its capacity. The April 26 attack, however, was unprecedented in its scale. Fake requests to communicate, running up to 50,000 hits per second, were used to strip the general public,s ability to access RFE as an information source. In doing so, the attackers also sought to mute the voices of hundreds of people who participate in RFE/RL,s online discussions, those who send their comments, questions, photos, and videos to this news source.

Sadly, we all know that this attack is not the first time that cyber aggression has been used in the OSCE region. We recall the cyber attack last year that was aimed at Estonia, in which still-unidentified perpetrators sought to disrupt government and commerce there, after a period of tension and controversy due to the attackers' dissatisfaction about one aspect of Estonian government policy.

Mr. Chairman, what occurred to RFE was a clear violation of guarantees of media freedom and of freedom of expression that the OSCE as an institution stands for, and which all 56 participating States are pledged to uphold. This new form of aggression, however, has even broader implications for security in the OSCE region. This emerging threat deserves further study. Such cyber attacks, whether or not they are undertaken with the acquiescence of a government, have the practical effect of denying people free access to information, and they must be condemned. Strategies are needed that strengthen our ability to defend ourselves against such threats.

The Anti-Terrorism Unit has examined to some degree terrorist use of the Internet, focusing on such issues as incitement

and recruitment. We believe the OSCE could perhaps examine the issue of cyber attacks and ways we can better defend legitimate information-sharing efforts from criminal attack. In the spirit of the initiative put forward by the Estonian delegation recently, we strongly recommend the Security Committee take a closer look at this issue and consider whether further work in this field is warranted for our organization.

Thank you, Mr. Chairman

End text
RICE